CPE™

cpe.mitre.org

Common Platform Enumeration (CPE)

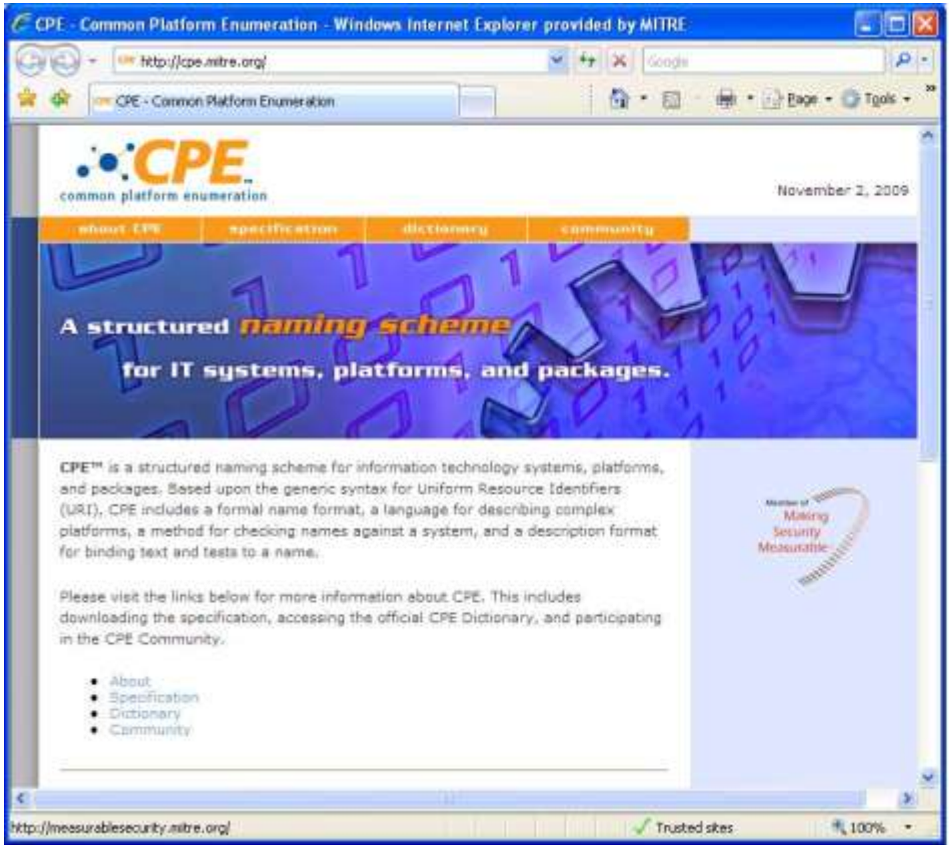
Introduction to the Standard

MITRE

What is CPE?

cpe.mitre.org

- CPE is:
  - A MITRE-led open standard
  - A structured naming scheme for IT products
  - Enabling technology for security automation
- CPE encompasses:
  - A prescribed name format
  - A language for describing complex platforms
  - A methodology for assigning canonical names
  - An algorithm for comparing names


CPE - Common Platform Enumeration - Windows Internet Explorer provided by MITRE
http://cpe.mitre.org/
Google
CPE - Common Platform Enumeration
Page
Tools
CPE
common platform enumeration
November 2, 2009
about CPE
specification
dictionary
community
A structured naming scheme
for IT systems, platforms, and packages.
Member of
Making Security Measurable
http://measurablesecurity.mitre.org/
Trusted sites
100%

CPE™ is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Please visit the links below for more information about CPE. This includes downloading the specification, accessing the official CPE Dictionary, and participating in the CPE Community.

- About
- Specification
- Dictionary
- Community

What Problem Does CPE Solve?

cpe.mitre.org

- Tremendous variation across the IT industry in how software and hardware products are named and versioned

- People have no difficulty interpreting the different marketing names that exist for each product, e.g.,
  - Microsoft Windows 2000
  - Win2K
  - Windows 5.0

- Machines cannot recognize that these three names all refer to the same product

- To achieve security automation objectives, a standardized name is needed for each platform

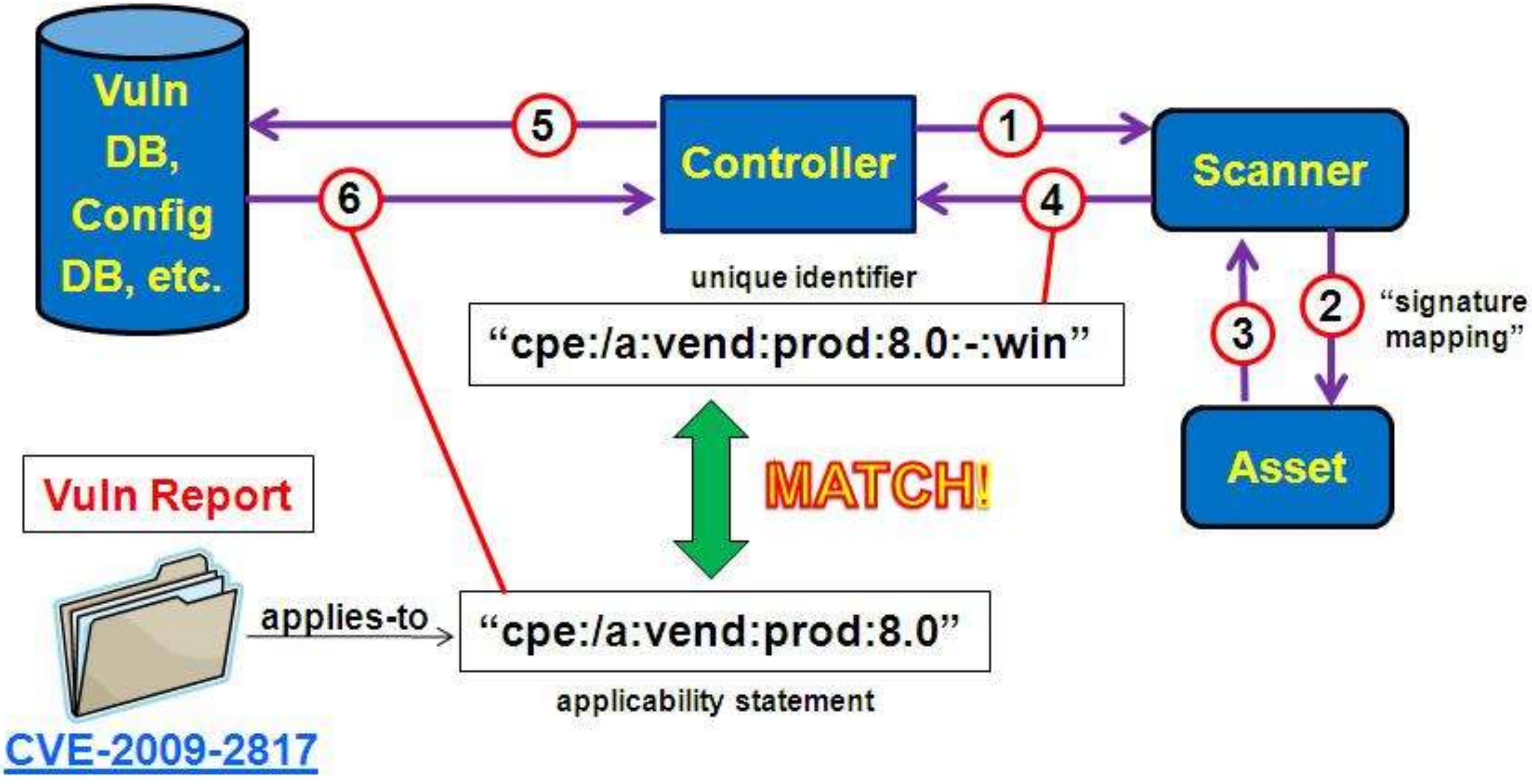
Technical Use Case Analysis

- Study performed in November 2008
  - To better understand the technical use cases
  - Interviewed members of the CPE Community
  - See: http://cpe.mitre.org/about/use_cases.html

- Four technical use cases were identified:
  - Software Inventory
  - Network-Based Discovery
  - Forensic Analysis/System Architecture
  - IT Management

- Software Inventory identified as a “must have”

CPE Concept of Operations



State of the Standard

- Current CPE version is 2.2
  - Specification published in March 2009
    - See: http://cpe.mitre.org/specification
  - Part of SCAP 1.0

- Draft version 2.3 released for public comment 26 Aug 2010
  - Implemented as three NIST Interagency Reports
    - Draft NIST IR 7695—Naming specification
    - Draft NIST IR 7696—Matching specification
    - Draft NIST IR 7697—Dictionary specification
  - See: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-XXXX (replace "XXXX" with the IR number)
  - Comment period closed 15 Sep 2010
  - Final drafts expected by end of 2010

Format of a CPE 2.2 Name

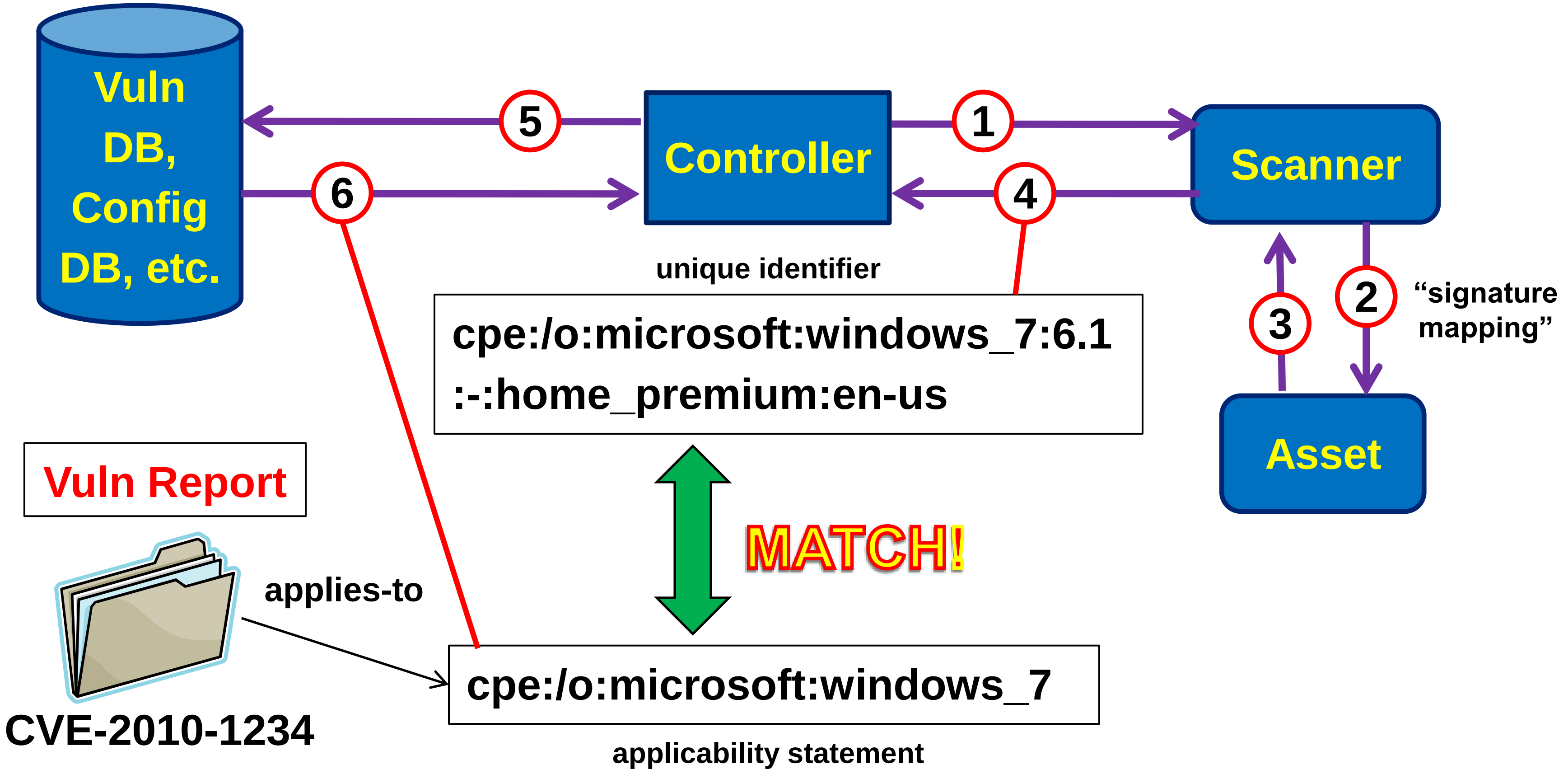
cpe:/ <part> :	*application, O/S, hardware*
<vendor> :	*vendor name*
<product> :	*product name*
<version> :	*product version*
<update> :	*update level of the product*
<edition> :	*edition of the product*
<language>	*internationalization*

Examples of CPE 2.2 Names

- cpe:/a:zonelabs:zonealarm_internet_security_suite:7.0
- cpe:/o:redhat:enterprise_linux:4:update5:ws
- cpe:/h:intel
- cpe:/a:jon_smith:tool_name:1.2.3
- cpe:/a:adobe:reader

CPE Matching (1 of 2)

cpe.mitre.org



Vuln DB, Config DB, etc.

Controller

Scanner

Asset

1

2

3

4

5

6

"signature mapping"

unique identifier

cpe:/o:microsoft:windows_7:6.1 :-:home_premium:en-us

MATCH!

Vuln Report

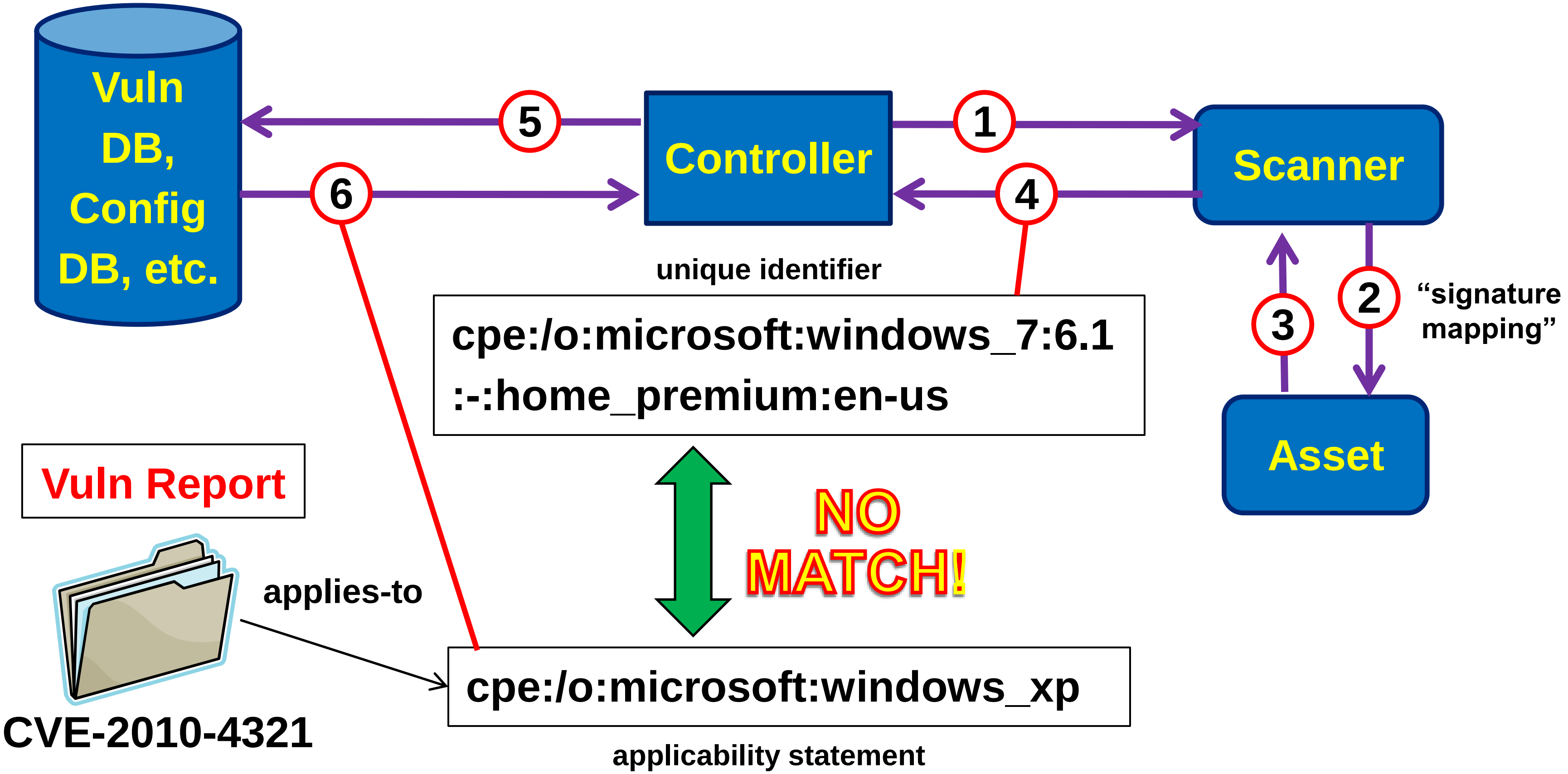
applies-to

CVE-2010-1234

cpe:/o:microsoft:windows_7

applicability statement

CPE Matching (2 of 2)



cpe:/o:microsoft:windows_7:6.1 :-:home_premium:en-us

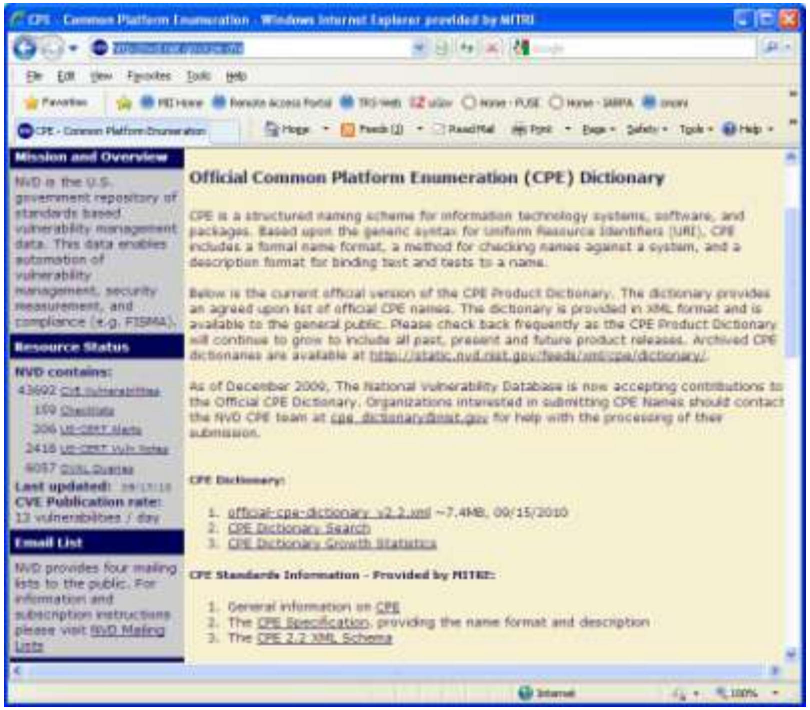
cpe:/o:microsoft:windows_xp

applicability statement

CPE Official Dictionary

CPE cpe.mitre.org

- Maintained by NIST
  - Part of the National Vulnerability Database
  - See: http://nvd.nist.gov/cpe.cfm
- New entries accepted by e-mail
  - cpe_dictionary@nist.gov
- ~ 24K entries as of 9/15/10
  - ~ 422 new entries per month Jan-Aug 2010 (average)


CPE - Common Platform Enumeration - Windows Internet Explorer provided by MITRE
File Edit View Favorites Tools Help
Favorites
CPE - Common Platform Enumeration
Page Feeds (1) Read Mail Print Page Safety Tools Help
Internet
100%

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
43692 CVE Vulnerabilities
199 Checklists
206 US-CERT Alerts
2418 US-CERT Vuln Notes
6057 OVAL Queries
Last updated: 09/17/10
CVE Publication rate:
13 vulnerabilities / day

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. Archived CPE dictionaries are available at http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

CPE Dictionary:

1. official-cpe-dictionary_v2.2.xml ~7.4MB, 09/15/2010
2. CPE Dictionary Search
3. CPE Dictionary Growth Statistics

CPE Standards Information - Provided by MITRE:

1. General information on CPE
2. The CPE Specification, providing the name format and description
3. The CPE 2.2 XML Schema

Example Dictionary Entries

```
<cpe-item name="cpe:/a:adobe:acrobat:9.3.3">
  <title xml:lang="en-US">Adobe Acrobat 9.3.3</title>
</cpe-item>


<cpe-item name="cpe:/o:microsoft:windows_7:-:-:x64">
  <title xml:lang="en-US">Microsoft Windows 7 64-bit</title>
  <notes xml:lang="en-US">
    <note>This CPE Name represents version 6.1.7600 of
          the Windows OS</note>
  </notes>
</cpe-item>
```

Summary

- CPE is a MITRE-led open industry standard for naming IT products (applications, operating systems, and hardware)

- Four elements to the standard:
  - A prescribed name format
  - A language for describing complex platforms
  - A methodology for assigning canonical names
  - An algorithm for comparing names

- Current version is 2.2—new release 2.3 coming soon

- Resources:
  - http://cpe.mitre.org
  - http://nvd.nist.gov/cpe.cfm